

**WHAT IS CLAIMED IS:**

1           1. A method for encrypting data in an access virtual private network (VPN), comprising the  
2 steps of:

3           performing a link control protocol (LCP) negotiation regarding at least one of an  
4 authentication method, data compression, maximum data size receivable, link status monitoring, and  
5 whether to perform data encryption;

6           checking a user identification (ID) and a password when the LCP negotiation determines that  
7 mutual authentication is required, said negotiation being conducted by two terminals according to  
8 an LCP negotiation condition at the step of performing the LCP negotiation;

9           performing data encryption when the step of performing the LCP negotiation results in a  
10 determination that data encryption is to be performed;

11          performing network control protocol (NCP) negotiation in order to negotiate information for  
12 a Layer 3 communication access between a user and a private network; and

13          transmitting and receiving data by forming a session between the user and the private  
14 network when the NCP negotiation is performed between the user and the private network.

1           2. The method according to claim 1, wherein the NCP negotiation is performed after the data  
2 encryption is performed.

1           3. The method according to claim 1, wherein the NCP negotiation is performed when it is  
2           determined, during performance of the LCP negotiation, that authentication and data encryption are  
3           not required.

1           4. The method according to claim 1, wherein an item for selecting whether to perform data  
2           encryption is added to an LCP negotiation option table of the user and the private network in advance  
3           of the step of performing the LCP negotiation.

1           5. The method according to claim 1, wherein the step of checking the user ID and the  
2           password comprises using a password authentication protocol (PAP) for providing user  
3           authentication by delivering the user ID and the password in form of a text.

1           6. The method according to claim 1, wherein the step of checking the user ID and the  
2           password comprises using a challenge handshake authentication protocol (CHAP) for providing user  
3           authentication using a hash function.

1           7. The method according to claim 1, wherein the step of performing data encryption  
2           comprises using a data encryption standard (DES).

1           8. The method according to claim 1, wherein the step of performing data encryption  
2 comprises using a user password as a key value for encryption.

1           9. The method according to claim 1, wherein the LCP negotiation is performed with respect  
2 to both the authentication method and whether to perform data encryption.

1           10. The method according to claim 9, wherein the step of performing data encryption  
2 comprises using a user password as a key value for encryption.